WHAT IS CLAIMED IS:

1. A method for negotiating a set of security parameters usable by an initiator and a responder to create a secure path over a network for exchanging information, the method including a plurality of modes, comprising:

conducting a main mode negotiation for establishing the secure path and selecting the set of security parameters including a security protocol;

conducting a quick mode negotiation for deriving a set of keys usable with the security protocol;

wherein at least a portion of the quick mode occurs during the main mode and a quick mode pseudo random number is exchanged between the responder and the initiator; and wherein a protocol security process establishes inbound and outbound protocol security associations.

2. The method of claim 1, further comprising:

conducting a first user mode for authenticating a first user associated with the initiator or responder.

3. The method of claim 2, wherein the initiator and the responder exchange authentication data that is calculated by application of a hash function incorporating a secret key on data exchanged during the main mode.

4. The method of claim 2, further comprising:

conducting a second user mode for authenticating a second user associated with the initiator or the responder.

5. The method of claim 1, wherein the main mode comprises:

sending, from the initiator to the responder, a set of proposed security parameters and authentication data;

selecting, by the responder, the set of security parameters from the set of proposed security parameters;

sending the set of security parameters from the responder to the initiator.

6. The method of claim 1, wherein the initiator identifies a public key of the responder prior to the main mode negotiation and wherein at least a portion a first message sent from the initiator to the responder is encrypted using the public key.

7. The method of claim 1, wherein the main mode comprises:

sending a group advertisement from the initiator to the responder; and

comparing the group advertisement to a set of authorized groups; and

sending a response from the responder to the initiator.

8. The method of claim 1, further comprising:

exchanging Diffie Hellman key data between the initiator and the responder during main mode for deriving keys for use with an encryption algorithm.

9. The method of claim 1, further comprising:

exchanging a pair of notify payloads between the initiator and the responder; wherein the pair of notify payloads are used by the protocol security process for establishing the protocol security associations.

10. A method for a first computer to dynamically discover a security policy of a second computer, wherein the first computer and the second computer are communicatively coupled to a computer network, comprising:

receiving, at the second computer, a request message from the first computer, wherein the request fails to conform to the security policy of the second computer;

sending, from the second computer to the first computer, a response message with a payload that identifies a subset of the security policy of the second computer; and

initiating, by the first computer, a security negotiation by sending a message including a proposed set of security parameters conforming to the security policy of the second computer.

11. The method of claim 10, wherein the request message is a standard IP packet with a clear text payload.

12. The method of claim 10, wherein the second computer is a responder and the first computer is an initiator, the initiator and the responder being in a main mode negotiation process and wherein the request message is sent from the initiator to the responder and includes one or more proposed security associations that fail to conform to the security policy of the responder.

13. The method of claim 10, wherein the second computer is an initiator and the first computer is a responder, the initiator and the responder being in a main mode negotiation process and wherein the request message is sent from the responder to the initiator and includes certificate data that fails to conform to the security policy of the initiator.

14. The method of claim 10, wherein the response message further includes an R-Cookie value used to prevent a denial of service attack, and the first computer includes a stateful firewall filter that permits the response message and blocks unsolicited packets received over the computer network.

15. A method for executing a security policy at a first network device wherein the first network device is communicatively coupled to a second network device over a computer network, comprising:

initiating a first security negotiation at the first network device by sending a first message with a first proposed set of security parameters;

determining, at the first network device, that the first security negotiation is unsuccessful and identifying a basis for the unsuccessful security negotiation;

initiating a second security negotiation, at the first network device by sending a second message with a second set of proposed security parameters.

16. The method of claim 15 wherein the unsuccessful security negotiation results from the first set of security parameters failing to conform to a security policy of the second network device and wherein the second set of proposed security parameters conform to the security policy of the second network device.

17. The method of claim 15 wherein the unsuccessful security negotiation results from a first certificate sent from the responder to the initiator, wherein the first certificate is invalid, the second security negotiation further comprising:

sending a certificate request from the initiator to the responder that includes an identification payload requesting a second certificate from the responder such that the second certificate is distinct from the first certificate.

18. A computer-readable medium for executing computer-readable instructions for negotiating a set of security parameters usable by an initiator and a responder to create a secure path over a network for exchanging information, the method including a plurality of modes, comprising:

conducting a main mode negotiation for establishing the secure path and selecting the set of security parameters including a security protocol;

conducting a quick mode negotiation for deriving a set of keys usable with the security protocol;

wherein at least a portion of the quick mode occurs during the main mode and a quick mode pseudo random number is exchanged between the responder and the initiator; and wherein a protocol security process establishes protocol security associations.

19. The computer-readable medium of claim 18, further comprising:

conducting a user mode for authenticating one or more users associated with the initiator or the responder.

20. The computer-readable medium of claim 19, wherein the initiator and the responder exchange authentication data that is calculated by application of a hash function incorporating a secret key on data exchanged during the main mode.

21. The computer-readable medium of claim 18, wherein the initiator identifies a public key of the responder prior to the main mode negotiation and wherein at least a portion a first message sent from the initiator to the responder is encrypted using the public key.

22. The computer-readable medium of claim 18, wherein the main mode comprises:

sending a group advertisement from the initiator to the responder;

comparing the group advertisement to a set of authorized groups; and

sending a response from the responder to the initiator.

23. A computer-readable medium for executing computer-readable instructions for executing a security policy at a first network device wherein the first network device is communicatively coupled to a second network device over a computer network, comprising:

initiating a first security negotiation at the first network device by sending a first message with a first proposed set of security parameters;

determining, at the first network device, that the first security negotiation is unsuccessful and identifying a basis for the unsuccessful security negotiation;

initiating a second security negotiation at the first network device by sending a second message with a second set of proposed security parameters.

24. The computer-readable medium of claim 23, wherein the unsuccessful security negotiation results from the first set of security parameters failing to conform to a security policy of the second network device and wherein the second set of proposed security parameters conform to the security policy of the second network device.

25. The computer-readable medium of claim 23, wherein the unsuccessful security negotiation results from a first certificate sent from the responder to the initiator, wherein the first certificate is invalid, the second security negotiation further comprising:

sending a certificate request from the initiator to the responder that includes an identification payload requesting a second certificate from the responder such that the second certificate is distinct from the first certificate.